CONTENTS

Acknowledgement i-ii
Preface iii-vi
Table of Cases vii-xi
Abbreviations xii-xv

CHAPTER ONE

INTRODUCTION 1-41
I. History and Evolution of Cyber Laws 04
II. Meaning and Definitions 08
A. Computer Crime 09
B. Computer Related Crime 10
C. Information Technology Crime 10
D. Telecommunication Crime 11
E. Cyber Crime 11
F. Cyber Law 12
III. Position Under American Law. 13
IV. Position Under English Law. 24
V. Position Under Australian Law. 31
VI. Position Under Indian law. 35

CHAPTER TWO

Nature Forms and Regulations of Cyber Space and Cyber Crimes 42-97
I. Introduction 42
II. Nature of Cyber Space. 43
A. Sophistication, Speed and Accuracy 44
B. Diversity and Plurality in Victimisation 45
C. Home to Global Vulnerabilities 46
III. Forms of Cyber Crimes. 48
A. Crime affecting Individuals. 49
i. Infringement of Privacy 49
ii. Identity Theft 53
iii. Cyber Stalking 55
B. Crime affecting Economy. 57
i. Hacking 58
ii. Virus and Other Malicious Programs 63
iii. Computer Sabotage and Computer Extortion 67
iv. Computer Fraud 68
v. Computer Forgery and Counterfeiting 71
vi. Theft of Telecommunication Services 72
vii. Software Piracy and other Copyright violations 74
viii. Economic Espionage 76
ix. Electronic Money Laundering and Tax Evasion 77
x. Cyber Squatting 79
C. Crime affecting National Security 80
i. Cyber Terrorism 80
ii. Cyber Warfare 83
D. Contents based crimes. 83
i. Racial and other hate propaganda 83
ii. Child Pornography 84

IV. Legal regulation of Cyberspace 86
A. Real world and Virtual world 86

V. Legal Regulation in Real World 89
A. Geographical Determinacy 89
B. Territorial Enforcement 89
C. Notion of Property 90
D. Paper Based Transaction 91
E. Real Relationship 91

VI. Legal regulation in Cyber World 92
A. World without Boundaries 92
B. Enforcement cannot be Territorial but global 94
C. Property is Notional 95
D. Virtual Relationship 97
E. Digitized Records 97

CHAPTER THREE
Global Legal Concerns and issues in Cyber Space 98-194
I. Domain Names 98
A. ICANN’s Uniform Domain Name Dispute Resolution Policy 99
B. The UDRP:- Global Perspective 101
C. Infringement of Trademarks in Online Medium-An Indian Perspective 106
i. Establishing a Prima facie Case 108
ii. Test of Acquired Distinctiveness 111

II. Network Service Provider 115
A. Meaning of Network Service Provider 115
B. Network Access Service Provider 116
C. Network Intermediary 116
D. Information Carrier 117
E. Information Publisher 117

III. Overview of ISP’s Liability 118
A. ISP’s Liability in the US 118
B. ISP’s Liability in the UK 122
C. ISP’s Liability in the EC 124
D. ISP’s Liability in India 126

IV. Freedom of Expression in Cyberspace 129
A. Position in US 130
B. Freedom of Expression and the Indian Constitution
   i. Reasonable Restriction 133
C. Freedom of Expression and the Internet 135

V. Spamming 138
A. Introduction 138
B. Position in America 140
C. Position in Australia 143
D. Position in United Kingdom 145
E. Position in India 147

VI. Computer Hacking 149

VII. Cyber Defamation 155
A. Introduction 155
B. Issues in Online Defamation 156
   i. Ingredients of Defamation 156
      a) Publication 157
C. Position under American Law 158
D. Position under English Law 160
E. Position under Australian Law 162
F. Whose Liability:- ISP or Website Promoter? 166
G. Future of Defamation in Cyberspace 169
H. Online Defamation:- An Indian Perspective 173

VIII. Obscenity 177
A. Introduction 177
B. Test for Obscenity in US 178
C. Test for Obscenity in India 181
D. Position under UK Law 185
E. Position under Indian Law 188
   i. Punishment U/S 67 IT Act 2000 191
   ii. Punishment U/S 292 IPC 1860 192
CHAPTER FOUR
Cyber Crimes & Jurisdictional Problem

I. Meaning of Jurisdiction.
   A. Prescriptive Jurisdiction.
   B. Enforcement Jurisdiction.

II. International Law.
   A. Territorial Principle.
   B. Nationality Principle.
   C. Protective Principle.
   E. The “Effective Doctrine” Principle
   F. Universality Principle.

III. International Law and State Law.
   A. Application of International Law by Courts
   B. Application of International law by International tribunals

IV. Jurisdiction in Cyber Space.
   A. Convention on Cyber Crime.
   B. Extraditable offences.
   C. Cyber Crimes and the issue of extradition.

V. The U.S. Approach to Personal Jurisdiction.
   A. Personal Jurisdiction.
   B. General Jurisdiction
   C. Specific Jurisdiction
   D. Enactment of Long arm statute
   E. Due process of Law
   F. Establishing Personal Jurisdiction in Cyber Space.
      i. Nature of Website
      ii. Interactive ‘Mixed’ Website
      iii. Passive website

VI. The Limit of Interactivity Criteria

VII. Jurisdiction on the Basis of Online Contract

VIII. Jurisdiction Based on Location of a Web Server

IX. European Approach to Personal Jurisdiction.
   A. The Brussels Regulation
   B. The Rome Convention

X. Indian Approach to Personal Jurisdiction
   A. Jurisdiction based on Forum of Choice
CHAPTER FIVE

Prevention of Cyber Crimes: International Initiatives 264-329

I. Introduction. 264
II. OECD Initiatives 266
III. G7 and G8 Groups 271
   A. P8 Expert Group on Misuse of International Data Networks 271
   B. High Tech Subgroup of G-8’s Senior Experts. 274
   C. G-8 conference on Dialogue between the Public Authorities and Private sector on security and trust in cyber space. 275
IV. Council of Europe Initiatives. 276
V. Conventions of Council of Europe 277
   A. Protection of Individuals with regard to Automatic Processing of Personal Data 277
   B. Council of Europe convention on cyber crimes, Budapest, 23 November 2001. 281
VI. Efforts of U.N. 291
VII. World Trade Organisation (WTO). 294
VIII. World Intellectual Property Organisaiton (WIPO) 296
IX. INTERPOL 297
X. National Police Organisation. 300
XI. Industry Driven Measures. 301
XII. Need for International Assistance in Cyber Crime 302
   Justice Administration.
   A. Issue of Extradition. 303
XIII. Cyber Statutes in Various countries. 306
   A. Austria 306
   B. Belgium 309
   C. Peoples Republic of China 311
   D. Estonia 315
   E. Germany 316
CHAPTER SIX
Prevention of Cybercrimes: Statutory Provisions in India

I. Introduction
II. Information Technology Act, 2000
III. Offences and Penalties
   A. Penalty for Damage of Computer, Computer System etc.
   B. Failure to Furnish Information, Return etc.
   C. Residuary Penalty
   D. Offence of Tampering with Computer Source Documents
   E. Offence of Hacking
   F. Offence of Obscene Publication
   G. Failure to Comply with Instruction from Controller
   H. Offence of Misrepresentation
   I. Breach of Confidentiality and Privacy
   J. Offence of Publishing Digital Signature false in Certain Particulars
   K. Publication for Fraudulent Purposes
IV. Subsidiary Provisions
   A. Application of Act to Offences Committed outside India
   B. Confiscation
   C. Penalties or Confiscation not to interfere with other punishments
   D. Power to Investigate Offences, Enter, Search etc.
   E. Offences by Companies
   F. Liability of Network Service Providers
V. Unresolved Issues
   A. Inapplicability
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.</td>
<td>Qualification for Appointment as Adjudicating Officers not prescribed</td>
</tr>
<tr>
<td>C.</td>
<td>Definition of Hacking</td>
</tr>
<tr>
<td>D.</td>
<td>No Steps to combat Internet Piracy</td>
</tr>
<tr>
<td>E.</td>
<td>Lack of International Cooperation</td>
</tr>
<tr>
<td>F.</td>
<td>Power of Police to Enter and search limited to public places</td>
</tr>
<tr>
<td>G.</td>
<td>Absence of Guidelines for investigations of Cybercrime.</td>
</tr>
<tr>
<td>VI.</td>
<td>Amendments to the Indian Penal Code 1860</td>
</tr>
<tr>
<td>VII.</td>
<td>Amendments to the Indian Evidence Act 1872</td>
</tr>
<tr>
<td>A.</td>
<td>Opinion as to digital signature where relevant</td>
</tr>
<tr>
<td>B.</td>
<td>Special Provisions as to evidence relating to electronic record</td>
</tr>
<tr>
<td>C.</td>
<td>Proof as to Digital signature</td>
</tr>
<tr>
<td>D.</td>
<td>Proof as to verification of Digital signatures</td>
</tr>
<tr>
<td>E.</td>
<td>Presumption as to electronic records and digital signature</td>
</tr>
<tr>
<td>F.</td>
<td>Presumption as to digital signature certificates</td>
</tr>
<tr>
<td>VIII.</td>
<td>Amendments to the Banker’s Books Evidence Act 1891</td>
</tr>
<tr>
<td>IX.</td>
<td>Amendment to the Reserve Bank of India Act 1934</td>
</tr>
<tr>
<td>A.</td>
<td>A Proactive Legislation</td>
</tr>
<tr>
<td>B.</td>
<td>One act syndrome</td>
</tr>
<tr>
<td>C.</td>
<td>Role of Judiciary</td>
</tr>
<tr>
<td>D.</td>
<td>Assimilating Technology</td>
</tr>
<tr>
<td>E.</td>
<td>Bridging a Digital Divide</td>
</tr>
<tr>
<td></td>
<td>Concluding Remarks</td>
</tr>
<tr>
<td>CHAPTER SEVEN</td>
<td>Conclusion and Suggestions 380-418</td>
</tr>
<tr>
<td>I.</td>
<td>Conclusion 380</td>
</tr>
<tr>
<td>II.</td>
<td>Suggestions 402</td>
</tr>
<tr>
<td></td>
<td>Bibliography xvi-xix</td>
</tr>
</tbody>
</table>